ISSN:0975-9646

Privacy Protection over Network Communication in Manet

[1]Dr.K.Rajangam .,
Head of EEE Department,
SCAD Institute of Technology

[2]Ms.L.Dhanam ,
Assistant Professor
Department of Computer Science & Engineering,
SCAD Institute of Technology

[3] Ms.Anuradha Balasubramanian
Assistant Professor
Department of ECE,Info Institute of Technology

Abstract **- The existing system introduces efficient privacy preserving routing protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature in which each node obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme. The USOR scheme is protect packet's content independent of traffic pattern unobservability which can be used with appropriate traffic padding schemes to achieve truly communication unobservability. Although it performs well wormhole attacks cannot be prevented in USOR mechanism. The proposed system aimed at developing unobservable routing scheme resistant against DoS attacks such as Gray hole/Black hole attacks to protect network-layer reactive protocols. It discovers malicious nodes during route discovery process when they mitigate fabricated routing information to attract the source node to send data through malformed packet.**

Keywords **- Routing protocols, malicious detection, Security.**

I.INTRODUCTION

A MANET is a decentralized network consisting of set of mobile nodes communicates with each other in shared wireless medium. Each node has limited communication range in the network and acts as a router to forward packets to another node.These topology changes rapidly which is unpredictable over time due to the mobility of the nodes. This arise the need of incorporating the routing functionality into nodes.

In such MANET privacy protection on routing is more challenging than that of wired networks due to dynamic nature and mobility of wireless media. A number of privacy preserving routing schemes has been established. However existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET which exploit asymmetric feature of public key cryptosystems to achieve their goals. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection.

Existing schemes fail to protect all content of packets from attackers. So that attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets which break unlinkability and may lead to source trace back attacks.

An attacker can mount traffic analysis based on packet type. In order to make the traffic content completely unobservable to outside attackers hide the information on packet type and node identity which is more critical to achieve. Mor over stronger decryption is provided in each encrypted packet to remove linkability. But it incurs high computational overhead which rely on public key cryptography. Among these requirements unobservability is the strongest one in that it implies not only anonymity but also unlinkability. To achieve unobservability a routing scheme should provide unobservability for both content and traffic pattern.

MANETs are vulnerable to various types of DoS attacks on network layer. In specific Gray hole and Black hole attacks malicious nodes deliberately disrupt data transmission in the network by sending\ incorrect routing information. These attacks disturb route discovery process and degrade network's performance. Thus it is a challenge to keep the communication route free from such attackers.

This paper proposes an efficient protocol to protect the network-layer reactive protocols from DoS attack. The proposed malicious node resistant scheme detects the malicious node sending false routing information. The routing packets are used not only to pass routing information but also to pass information about malicious nodes and detect the malicious node during route discovery process when they evade fabricated routing information to attract the source node to send data through itself.

The contribution of this paper includes (i) Establishes safe and secure communication. (ii) An unobservable secure routing scheme employing anonymous key establishment based on group signature. (iii) It provides strong privacy preserving routing for ad hoc networks and also resistant against attacks due to node compromise. The remainder of paper is organized as follows.

II. LITERATURE REVIEW

2.1 ANODR scheme:

Provide anonymity for routing in ad hoc network. It uses one-time public/private key pairs to achieve anonymity for route discovery. During the route discovery process, each intermediate node creates a one-time public/private key pair to encrypt/decrypt the routing, so as to break the linkage between incoming packets and corresponding outgoing packets. However, packets are publicly labeled and the attacker is able to distinguish different packet types which fail to guarantee unobservability.

2.2 ASR and ARMR scheme:

It is designed to achieve stronger location privacy than ANODR, which ensures nodes on route have no information on their distance to the source/destination node. It reduces computation burden on one-time public/private key pair generation. ARMR uses one-time public keys and bloom filter to establish multiple routes for MANETs.

2.3 SDAR and ODAR:

It uses long-term public/private key pairs at each node for anonymous communication. It is similar to ARM except ARM uses shared secrets between source and destination for verification. ODAR provides only identity anonymity since the entire RREQ/RREP packets are not protected with session keys.

2.4 MASK:

MASK requires a trusted authority to generate sufficient pairs of secret points and corresponding pseudonyms as well as cryptographic

parameters. It is vulnerable to key pair depletion attacks. The RREQ flag is not protected and this enables passive adversary to locate the source node and destination node's identity. Thus an adversary can easily recover linkability between different RREQ packets with the same destination which actually violates receiver anonymity.

2.5 An anonymous location-aided routing scheme ALARM:

The public key cryptography and the group signature are used to preserve privacy. The group signature has a good privacy preserving feature in that everyone can verify a group signature but cannot identify who is the signer. But ALARM still leaks sensitive privacy information such as network topology and location of every node. Hence public key cryptosystems have a preferable asymmetric feature and it is well-suited for privacy protection in MANET. However existing schemes provide only anonymity and unlinkability while unobservability is never considered.

III. EXISTING SYSTEM

An efficient unobservable routing scheme USOR is deployed in the existing system. In this protocol both control packets and data packets look random and in distinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption.The perception behind this scheme is that if a node can establish a key with each of its neighbours, then it can use such a key to encrypt the whole packet for a corresponding neighbour. The receiving neighbour can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are needed. As a result, USOR comprises two phases: anonymous trust establishment and unobservable route discovery. Both the group signature scheme and the ID-based scheme are based on pairing of elliptic curve groups of order of a large prime (e.g. 170-bit long) so that they have the same security strength as RSA algorithm.

Group signature scheme: The key server generates a group public key gpk which is publicly known by everyone, and a private group signature key gsk for each node X. The group signature scheme ensures full anonymity which means a signature does not reveal the signer's identity but everyone can verify its validity.

ID-based encryption scheme:

Groups with a bilinear map allow us to build public key encryption schemes with new properties whereas it is difficult for groups without a bilinear map. Public-key encryption scheme contains publicly-known string (e.g. someone's email address) which could be used as a public key. The corresponding private key is delivered to the proper owner of this string (e.g. the recipient of the email address) by a trusted private key generator. This key generator must verify the user's identity before delivering a private key. A user proves his identity in a lazy way, only once he needs his private key to decrypt a message sent to him.

Execution of Phases:

1. Anonymous key establishment process is performed to construct secret session keys.

2. Unobservable route discovery process is executed to find a route to the destination.

3.1 Anonymous key establishment

The messages exchanged in this phase are not unobservable, but this would not leak any private information like node identities. As a result of this phase, a pair wise session key is constructed anonymously, which means the two nodes establish this key without knowing who the other party is. Meanwhile, node S establishes a local broadcast key and transmits it to all its neighbours. It

is used for per-hop protection for subsequent route discovery. The protocol uses elliptic curve Diffie- Hellman (ECDH) key exchange and uses group signature.

3.2 Unobservable route discovery process

This phase is a privacy-preserving route discovery process based on the keys established in previous phase. It comprises of route request and route reply. The route request messages flood throughout the whole network while the route reply messages are sent backward to the source node only.

3.3 Traffic Pattern Unobservability

No useful information can be obtained from frequency, length, and source-destination patterns of message traffic. USOR protect all parts of a packet's content and it is independent of solutions on traffic pattern unobservability which is used with appropriate traffic padding schemes to achieve truly communication unobservability.

3.4 Disadvantages Of Existing System

- Wormhole attacks cannot be prevented in USOR mechanism.
- They require large keys that can only be used once.
- Low efficiency

IV PROPOSED SYSTEM

The challenging task of unobservable routing scheme is DoS attacks such as Gray hole and Black hole attacks in MANET cannot be detected. Those attacks contain malicious nodes which deliberately disrupt data transmission in the network by sending incorrect routing information. In order to keep the communication route free from such attackers the proposed approach employs a method for determining conditions under which malicious node should be monitored. It contains intermediate node which detects the malicious node sending false routing information as well as the routing information. Thus it not only detects but also removes malicious node by isolating it to make safe and secure communication. Apart from identification of malicious node, it has been observed that this approach leads less communication breakage in ad hoc routing. The experimental results demonstrate that the proposed approach can effectively detect malicious nodes.

In Black hole attack, the malicious node generates and propagates fabricated routing information and advertises itself as having a valid shortest route to the destined node. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. Therefore, packets do not reach to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, network traffic is absorbed. Gray hole attack is an extension of Black hole attack in which a malicious node's behaviour is exceptionally unpredictable. A node may behave maliciously for a certain time but later on it behaves just like other ordinary nodes. Both Black hole and Gray hole attacks disturb route discovery process and degrade network's performance.

Malicious node interruption:

Source node S broadcasts route request packet (RREQ). Nodes within its communication range A and C, receive the RREQ and rebroadcasts RREQ to their neighbours until a node having a valid route to the destination or destination D itself receives RREQ. This node sends RREP to the source node on the reverse path of RREQ. The malicious node M sends RREP with higher, but constructs sequence number to the source. Another RREP is sent by D having genuinely higher sequence number. As malicious node sends RREP with higher sequence number than the normal node, S chooses path through M to transfer data packets and therefore, malicious node can drop some or all received packets which causes disruption in network operations.

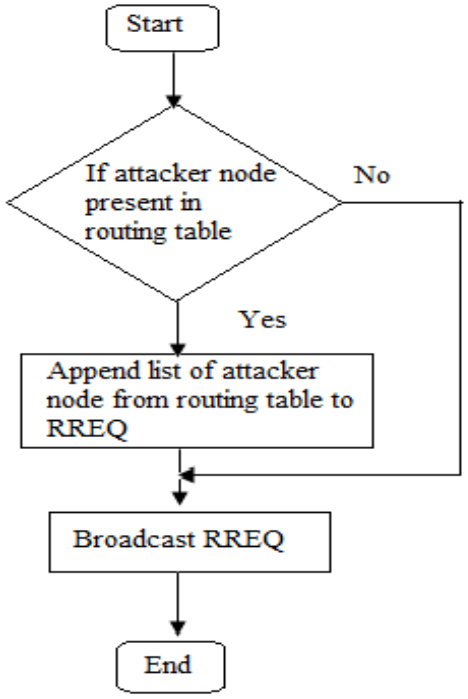

Fig: 1. system flow diagram for sending *RREQ*

Defense approach:

An intermediate node dynamically calculates a PEAK value after every time interval that uses three parameters for calculation such as RREP sequence number, routing table sequence number, number of replies received during the time interval.

The PEAK value is the maximum possible value of sequence number that any RREP can have in the current state. **RREP received** from malicious node is marked as **DO_NOT_CONSIDER.**

4.1 ADVANTAGES OF PROPOSED SYSTEM

- Integrated multicast routing
- We will get both unicast and multicast data
- Aggregation to be quite significant
- It reduces overhead for achieving security.
- The throughput is increased after eliminating malicious node detection.

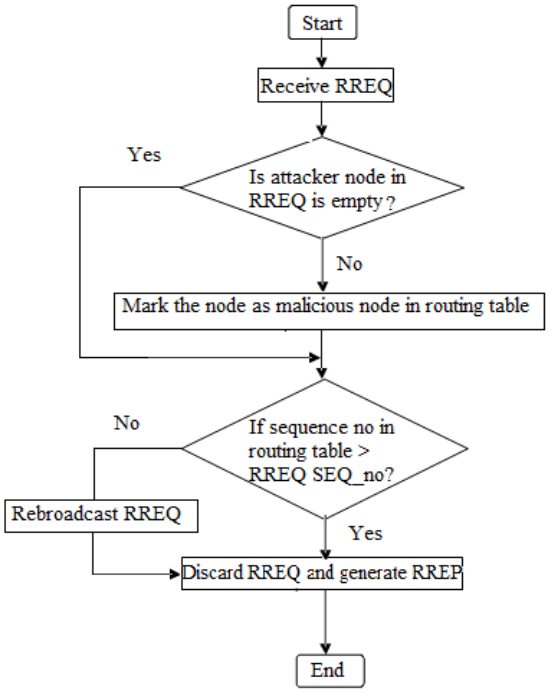

Fig: 2. System flow diagram for receiving RREQ

V IMPLEMENTATION RESULTS

The proposed algorithm detects and removes malicious nodes during the route discovery phase. Nodes receiving RREP verify the correctness of routing information. Source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets.As there is no extra control packets added in the proposed algorithm, there would be negligible difference in Routing Overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. Moreover as the malicious nodes would be isolated

Packet Delivery Ratio (PDR) would be improved greatly. PDR is the ratio of number of received data packets to the number of sent data packets. If the node receiving RREP from a malicious node doesn't have the node marked as malicious in the routing table the proposed algorithm adds a little computational overhead to that node as it has to calculate the PEAK value.

Enhanced USOR

Finally we compare USOR with enhanced USOR in terms of privacy protection. We alter the number of eavesdropping nodes in the network and compute the sender anonymity of RREQ packets. It can be seen from USOR provides best privacy protection than the existing USOR regardless of the number of eavesdroppers.

VI CONCLUSION AND FUTURE WORK

The unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks offers strong privacy protection with complete unlinkability and content unobservability for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection but also more resistant against attacks due to node compromise.

The proposed work defends against wormhole attacks which cannot be prevented with USOR. This make the unobservable routing scheme resistant against DoS attacks. The proposed algorithm detects and removes malicious nodes during the route discovery phase. Nodes receiving RREP verify the correctness of routing information. As there is no extra control packets added in the proposed algorithm, Packet Delivery Ratio (PDR) would be improved greatly as the malicious nodes are isolated.

More and more efficient routing protocols for MANET might come in front in the coming future which might take security and QoS (Quality of Service) as the major concerns. So far, the routing protocols mainly focused on the methods of routing, but in future a secured but QoS-aware routing protocol could be worked on. Ensuring both of these parameters at the same time might be difficult. A very secure routing protocol surely incurs more overhead for routing which might degrade the QoS level. So an optimal trade-off between these two parameters could be searched.

REFERENCES

[1] Zhiguo Wan, Kui Ren, and Ming Gu," USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks," IEEE transactions on wireless communications, vol. 11, no. 5, may 2012.

[2] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

[3] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in PET04, LNCS 3424, 2004, pp. 207–225.

[4] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. of the ACM, vol. 4, no. 2, Feb. 1981.

[5] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.

[6] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBI- HOC'03, pp. 291–302.

[7] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anony-mous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.

[8] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International

Conference on Advanced Information Networking and Applications, pp. 133–137.

[9] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33– 42.

[10] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536– 1550, 2009.